

AMENDMENTS TO CLAIMS

Please amend the claims as indicated hereinafter.

1. (Currently amended) A method, comprising the computer-implemented steps of:
in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
determining a user identifier associated with the network device that has caused a security event in the network;
in response to the security event, causing the network device to acquire a ~~new~~ second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;
wherein the second subset of addresses is different from the first subset of addresses; and
configuring one or more security restrictions with respect to the ~~new-second~~ network address.
2. (Original) A method as recited in Claim 1, further comprising the steps of:
receiving information identifying the security event in the network;
correlating the security event information with network user information to result in determining the user identifier associated with the network device.
3. (Currently Amended) A method as recited in Claim ~~1~~ 44, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the step of causing the network device to acquire the ~~new-second~~ network address

comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.

4. (Currently Amended) A method as recited in Claim ~~4~~ 44, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the step of causing the network device to acquire the ~~new-second~~ network address comprises issuing a DHCP FORCE_RENEW message to the network device.

5. (Currently Amended) A method as recited in Claim ~~4~~ 44, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the step of causing the network device to acquire the ~~new-second~~ network address comprises prompting the network device to request a new network address using DHCP.

6. (Currently Amended) A method as recited in Claim 1, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the step of causing the network device to acquire the ~~new-second~~ network address comprises waiting for expiration of a lease for a current network address of the network device.

7. (Currently Amended) A method as recited in Claim 1, wherein the step of causing the network device to acquire the ~~new-second~~ network address comprises the step of providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.

8. (Original) A method as recited in Claim 7, further comprising the step of publishing information describing characteristics of the special IP subnet to network service providers.

9. (Currently Amended) A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the ~~new-second~~ network address.

10. (Currently Amended) A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL

associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the ~~new-second~~ network address.

11. (Original) A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

12. (Previously presented) A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if not, removing the user from the second specified pool.

13. (Original) A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider.

14. (Currently Amended) A method, comprising the computer-implemented steps of:
in a security controller that is coupled, through a network, to a network device having a
first network address assigned from a first subset of addresses within a first
specified pool associated with normal network users;
receiving information identifying a security event in the network;
correlating the security event information with network user information to result
in determining a network user associated with the network device that
caused the security event;
in response to receiving the information identifying the security event, placing the
user in an elevated risk security group by causing the network device to
acquire a ~~new-second~~ network address that is selected from a second
subset of addresses within a second specified pool associated with
suspected malicious network users;
wherein the second subset of addresses is different from the first subset of
addresses;

configuring one or more security restrictions with respect to the ~~new-second~~
network address;
determining whether a malicious act caused the security event;
if a malicious act caused the security event, then providing information about the
security event or malicious act to a security decision controller;
if a malicious act did not cause the security event, then removing the user from
the elevated risk group.

15. (Canceled)

16. (Currently Amended) A method as recited in Claim 14, wherein causing the network device to acquire the ~~new-second~~ network address comprises the steps of:

re-configuring a dynamic host control protocol (DHCP) server to require said server to
issue any new network address to the network device only from a specified group
of network addresses that is reserved for users associated with elevated user risk;
and
performing any one of the steps of:

- (a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP;
- (b) issuing a DHCP FORCE_RENEW message to the network device;
- (c) prompting the network device to request a new network address using DHCP; or
- (d) waiting for expiration of a lease for the first network address of the network device.

17. (Currently Amended) A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:
modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the ~~new-second~~ network address; and
modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the ~~new-second~~ network address.

18. (Currently Amended) A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:
- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
- determining a user identifier associated with the network device that has caused a security event in the network;
- in response to the security event, causing the network device to acquire a ~~new~~ second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
- wherein the second subset of addresses is different from the first subset of addresses; and
- configuring one or more security restrictions with respect to the ~~new~~ second network address.
19. (Currently Amended) An apparatus, comprising:
- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
- means for determining a user identifier associated with the network device that has caused a security event in the network;
- means for, in response to the security event, causing the network device to acquire a ~~new~~ second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
- wherein the second subset of addresses is different from the first subset of addresses; and

means for configuring one or more security restrictions with respect to the ~~new~~
second network address.

20. (Currently Amended) An apparatus, comprising:
a network interface that is coupled to a data network for receiving one or more packet flows therefrom;
a processor;
one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
in a security controller that is coupled, through the data network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
determining a user identifier associated with the network device that has caused a security event in the network;
in response to the security event, causing the network device to acquire a ~~new~~
second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the second subset of addresses is different from the first subset of addresses; and
configuring one or more security restrictions with respect to the ~~new~~-second network address.

21–23. (Canceled).

24. (Currently Amended) A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
receiving information identifying a security event in the network;
correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event;
in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a ~~new~~-second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the second subset of addresses is different from the first subset of addresses;
configuring one or more security restrictions with respect to the ~~new~~-second network address;
determining whether a malicious act caused the security event;
if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller;
if a malicious act did not cause the security event, then removing the user from the elevated risk group.

25. (Currently Amended) An apparatus comprising:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
means for receiving information identifying a security event in the network;
means for correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event;

means for, in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a ~~new~~-second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein the second subset of addresses is different from the first subset of addresses;

means for configuring one or more security restrictions with respect to the ~~new~~ second network address;

means for determining whether a malicious act caused the security event;

means for, if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller;

means for, if a malicious act did not cause the security event, then removing the user from the elevated risk group.

26. (Currently Amended) An apparatus, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor; and

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

receiving information identifying a security event in the network;

correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event;

in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a ~~new~~-second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the second subset of addresses is different from the first subset of addresses;
configuring one or more security restrictions with respect to the ~~new~~-second network address;
determining whether a malicious act caused the security event;
if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller;
if a malicious act did not cause the security event, then removing the user from the elevated risk group.

27. (Canceled)

28. (Currently Amended) The apparatus of claim 26, wherein the instructions which when executed cause the network device to acquire a ~~new~~-second network address comprise further instructions which when executed cause:
- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk;
and
 - performing any one of the steps of:
 - (a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP;
 - (b) issuing a DHCP FORCE_RENEW message to the network device;
 - (c) prompting the network device to request a new network address using DHCP; or

- (d) waiting for expiration of a lease for the first network address of the network device.
29. (Currently Amended) The apparatus of claim 26, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:
- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the ~~new~~ second network address; and
- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the ~~new~~ second network address.
30. (Currently Amended) The apparatus of claim 20, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new~~ second network address, and wherein the instructions which when executed cause the network device to acquire a ~~new~~ second network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.
31. (Currently Amended) The apparatus of claim 20, wherein instructions which when executed cause the network device to acquire a ~~new~~ second network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.
32. (Currently Amended) The apparatus of claim 20, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new~~ second network address, and wherein the instructions which when executed cause the network device to acquire a ~~new~~ second network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device.

33. (Currently Amended) The computer-readable storage medium of claim 18, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the instructions which, when executed, cause the network device to acquire the ~~new-second~~ network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.
34. (Currently Amended) The computer-readable storage medium of claim 18, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the instructions which when executed cause the network device to acquire the ~~new-second~~ network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device.
35. (Currently Amended) The computer-readable storage medium of claim 18, wherein instructions which when executed cause the network device to acquire a ~~new-second~~ network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.
36. (Currently Amended) The apparatus of claim 19, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the means for causing the network device to acquire the ~~new-second~~ network address comprise means for resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.
37. (Currently Amended) The apparatus of claim 19, wherein the network device uses dynamic host control protocol (DHCP) to obtain the ~~new-second~~ network address, and wherein the means for causing the network device to acquire the ~~new-second~~ network address comprise means for issuing a DHCP FORCE_RENEW message to the network device.

38. (Previously Presented) The apparatus of claim 19, wherein the means for causing the network device to acquire a new network address comprise means for providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.
39. (Currently Amended) The computer-readable storage medium of claim 24, wherein the instructions which when executed cause the network device to acquire a new-second network address comprise further instructions which when executed cause:
re-configuring a dynamic host control protocol (DHCP) server to require said server to
issue any new network address to the network device only from a specified group
of network addresses that is reserved for users associated with elevated user risk;
and
performing any one of the steps of:
~~(a)~~(c) _____resetting a port that is coupled to the network device to trigger the network
device to request a new network address using DHCP;
~~(b)~~(f) _____issuing a DHCP FORCE_RENEW message to the network device;
~~(c)~~(g) _____prompting the network device to request a new network address using
DHCP; or
~~(d)~~(h) _____waiting for expiration of a lease for the first network address of the
network device.
40. (Currently Amended) The computer-readable storage medium of claim 24, wherein the instructions which when executed cause configuring one or more security restrictions
comprise instructions which when executed cause:
modifying an internet protocol (IP) access control list (ACL) associated with a port that is
coupled to the network device to permit entry of IP traffic from only the new-second
second network address; and
modifying a media access control (MAC) ACL associated with the port to permit entry of
traffic only for a MAC address that is bound to the new-second network address.

41. (Currently Amended) The apparatus of claim 25, wherein the means for causing the network device to acquire a new-second network address further comprise:
means for re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk; and
means for performing any one of the steps of:
~~(e)~~(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP;
~~(f)~~(b) issuing a DHCP FORCE_RENEW message to the network device;
~~(g)~~(c) prompting the network device to request a new network address using DHCP; or
~~(h)~~(d) waiting for expiration of a lease for the first network address of the network device.
42. (Currently Amended) The apparatus of claim 25, wherein the means for configuring one or more security restrictions comprise:
means for modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new-second network address; and
means for modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new-second network address.
43. (New) The method of Claim 1, wherein causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address.
44. (New) A method, comprising the computer-implemented steps of:

in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

in response to a security event in the network, causing the network device to acquire a second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;

wherein causing the network device to acquire a second network address comprises performing an action that causes the network device to request a new network address;

wherein the second subset of addresses is different from the first subset of addresses; and

configuring one or more security restrictions with respect to the new network address.